Polynomials with roots mod p for all primes p

J. Group Theory **4** (2001), 233–239

Journal of Group Theory

Polynomials with roots mod p for all primes p

Rolf Brandl, Daniela Bubboloni* and Ingrid Hupp

(Communicated by F. de Giovanni)

Abstract. Let $f(X)$ be an integer polynomial of degree m with no linear factors, and assume that its Galois group is the (most common) symmetric group S_n ($n \leqslant m$). If $f(X)$ has a root modulo p for all primes p, then $3 \leqslant n \leqslant 6$.

1 Introduction

Let $f(X)$ be a non-zero integer polynomial. We are interested in the roots of $f(X)$ modulo various primes p. Obviously, if $f(X)$ has a monic linear factor, then the congruence $f(x) \equiv 0 \bmod p$ has solutions for all p. However, there are polynomials without linear factors which enjoy the same property. The first example for this is due to Hilbert. Indeed, let $f(X) = (X^2+1)(X^2-2)(X^2+2)$, and let p be a prime. If both congruences $x^2 \equiv 2 \bmod p$ and $x^2 \equiv -2 \bmod p$ have no solutions, then 2 and -2 are non-squares modulo p. This implies that -4 is a non-zero square modulo p, whence the congruence $x^2 \equiv -1 \bmod p$ can be solved.

We shall be concerned with the question how many irreducible factors f must have at least, and what can be said about the Galois group G of f over the rationals. Note that the hypothesis on G in the theorem is a very mild one because, by [9], for almost all f, we have that G is a symmetric group.

Theorem. *Let $f(X)$ be an integer polynomial, and assume that f has a root modulo p for all primes p. If f is a product of l irreducible factors none of which is linear, then $l \geqslant 2$. If $l = 2$ and the Galois group of f over the rationals is isomorphic to the symmetric group S_n, then $3 \leqslant n \leqslant 6$.*

Thus the smallest interesting case is when $f(X)$ is a product of two irreducible factors over the integers. Here there is an example for this situation:

Example. Let $f(X) = (X^2+X+1)(X^3-2)$, and let p be a prime. If $p \not\equiv 1 \bmod 3$, then the order of the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$ is not divisible by 3. Hence 2 is a

*Work of the second author was supported by M.U.R.S.T. and G.N.S.A.G.A.

cube modulo p. If $p \equiv 1 \bmod 3$, then there exists a primitive cube root of unity x modulo p. This obviously is a root of the polynomial $X^2 + X + 1$, which is the third cyclotomic polynomial. Note that the Galois group of f is S_3.

All groups in this paper are finite. All unexplained notation is standard (see [6]). Given a non-empty set Ω, we denote the symmetric group on Ω by $\operatorname{Sym}\Omega$. When $\Omega = \{1, \ldots, n\}$ we use the simpler notation S_n. Similarly for the alternating groups A_n.

Many questions about factorization of $f(X)$ modulo p can be translated into properties of the Galois group G of $f(X)$ over the rationals. Using some results of Frobenius, the following can easily be proved:

Lemma 1.1 (see [2, Lemma 2]). *Let $g(X)$ be an irreducible integer polynomial, and let G be its Galois group over the rationals acting on the roots of g. Let p be a prime not dividing the discriminant of the splitting field of g. If $g(X) = \prod_{i=1}^{t} g_i(X) \bmod p$, where the g_i are irreducible modulo p, then G contains at least one permutation which is the product of t disjoint cycles of lengths $n_1, \ldots, n_t$, where n_i is the degree of g_i.*

Hence if f has a root modulo p for all primes p, then every permutation of G has at least one fixed point on the set Ω of the roots of f (note that this is not the natural action of S_n on n symbols). Choose one element ω_i in each orbit of G on Ω, and let U_i be the stabilizer of ω_i. Then G is the set-theoretic union of the conjugates of $U_1, \ldots, U_l$, where l denotes the number of irreducible facors into which $f(X)$ splits over the rationals. As $f(X)$ has no linear factor, all U_i are proper subgroups of G. Now the case $l = 1$ when $f(X)$ is irreducible can easily be eliminated:

Proposition 1.2. *Let $f(X)$ be an irreducible integer polynomial of degree > 1. Then there exists a prime p such that the congruence $f(x) \equiv 0 \bmod p$ cannot be solved.*

Proof. Otherwise, by the above discussion, there would exist a proper subgroup U of G such that $G = \bigcup_{g \in G} U^g$. However this implies that $G = U$, a contradiction.

In this paper, we analyse the case when $l = 2$. To do this, we first introduce a definition. The finite group G is called *coverable*, if there exist two proper subgroups U_1, U_2 of G such that G is the set-theoretic union of the G-conjugates of U_1 and U_2. This notion was introduced by the second author in [3]. Coverings by one subgroup, under the action of the whole automorphism group A of G, have been discussed by the first author [1] and Praeger et al. (see [7], [8]) in the more general context where $\operatorname{Inn}(G) \leqslant A \leqslant \operatorname{Aut}(G)$.

2 Some small values for *n*

In this section we record some basic facts on coverings of symmetric groups, some examples that can be covered by conjugates of two proper subgroups, and some which cannot.

If the element $\sigma \in S_n$ decomposes into a product of disjoint cycles $\sigma_1, \ldots, \sigma_k$ of lengths $l_1, \ldots, l_k \geqslant 2$, we will say that the *type* of σ is $t = [l_1; \ldots; l_k]$. Observe that we omit the lengths equal to 1. If a subgroup U of S_n contains at least one permutation of type t, we shall write $t \in U$. Otherwise, we write $t \notin U$. For example, $[n] \notin U$ means that U does not contain any cycle of length n.

It is well known that two elements of S_n are conjugate if and only if they are of the same type. This proves the following basic result:

Lemma 2.1. *Let $G = S_n$, and let U_1 and U_2 be proper subgroups of G. Then U_1 and U_2 define a covering of G if and only if each type of permutation appears at least once either in U_1 or in U_2.*

As a first application of (2.1), we present some symmetric groups that can be covered by the conjugates of two proper subgroups:

Remark 2.2. The groups S_n are coverable for $3 \leqslant n \leqslant 6$.

Proof. The covering of S_3 is obvious. In the case of S_4 we can choose for U_1 the stabilizer of one point, and for U_2 a Sylow 2-subgroup of S_4. For $G = S_5$, let $U_1 = G_{\{1,2\}}$ and $U_2 = N_G\langle(12345)\rangle$. Then U_2 contains permutations of the types [4], [5], [2; 2]. Moreover U_1 contains permutations of the types [2], [3], [2; 3]. Hence, by (2.1), the subgroups U_1 and U_2 define a covering of G.

For $G = S_6$, let U_1 be the stabilizer in G of the partition $\{1, 2, 3\}$, $\{4, 5, 6\}$ and let $U_2 = S_5$. Then U_1 contains the permutation (142536) of type [6], and therefore also a permutation of type [2; 2; 2] and one of type [3; 3]. Moreover U_1 contains the permutation (14)(2536) of type [2; 4]; hence for each type of fixed-point-free permutation, the subgroup U_1 contains at least one representative. On the other hand U_2 contains representatives for each type of permutation with at least one fixed point, and again (2.1) applies.

To prove that a given group cannot be covered, it is often possible to show that one of the subgroups U_1, U_2 has to be primitive. In many cases, the following can be applied:

Lemma 2.3 ([10], 13.9). *Let $G \leqslant S_n$ be a primitive group, and let p a prime such that $p \leqslant n - 3$. If G contains a p-cycle, then $G \geqslant A_n$.*

Lemma 2.4. *The groups S_7 and S_8 cannot be covered.*

Proof. Let U_1 and U_2 define a covering of S_7. Without loss of generality, let U_1 contain a 7-cycle. Then, as 7 is a prime, U_1 is primitive and, by (2.3), we get $[2] \notin U_1$. However U_2 cannot be primitive, because otherwise, since $[2] \in U_2$, by 2.3 again, we would have $U_2 = S_7$. This implies that U_2 is not transitive, and therefore we can

assume that

$$U_2 = \mathrm{Sym}\{1, \ldots, a\} \times \mathrm{Sym}\{a+1, \ldots, 7\}$$

where a denotes the minimal length of an orbit of U_2. Obviously, $1 \leqslant a \leqslant 3$.

If $a = 1$ or $a = 3$, then U_2 contains no permutations of type $[2;5]$, and hence there exists $\mu \in U_1$ of this type. Consequently the transposition μ^5 belongs to U_1, and we can again appeal to (2.3) to conclude that $U_1 = S_7$.

If $a = 2$, we have that $U_2 = \mathrm{Sym}\{1,2\} \times \mathrm{Sym}\{3,4,5,6,7\}$ contains no permutations of types $[6]$ and $[3;4]$. Therefore U_1 contains at least one permutation of type $[6]$ and one permutation μ of type $[3;4]$. Then $U_1 \neq A_7$, $\mu^4 \in U_1$ is a 3-cycle, and (2.3) leads to the contradiction $U_1 = S_7$.

Next, let U_1 and U_2 define a covering of S_8 where U_1 contains a 7-cycle. If U_1 is not transitive, then we may assume that $U_1 = S_7$ and U_2 contain all types of permutations with no fixed points. In particular, U_2 contains at least one permutation of the types $[8]$, $[5;3]$ and $[3;3;2]$. Since U_2 is transitive and 5 divides $|U_2|$, we conclude that U_2 is primitive. As U_2 contains a transposition, by (2.3), we obtain that $U_2 = S_8$.

Hence U_1 is transitive, and indeed 2-transitive. We observe that U_1 contains neither 3-cycles nor 5-cycles. Namely, if we assume the contrary, then by (2.3), we must have $U_1 = A_8$; yet this implies that U_2 contains all types of odd permutations, and in particular U_2 contains an 8-cycle and permutations of the types $[3;4]$ and $[6]$. Hence U_2 is 2-transitive and, since it contains transpositions, we deduce that $U_2 = S_8$.

In particular, U_1 contains no permutation of the types $[3;5]$, $[3;4]$ and $[2;5]$. Hence U_2 contains at least one permutation of these types. Next observe that U_2 cannot be transitive, because otherwise the stabilizer $(U_2)_1$ would contain permutations of the types $[3;4]$, $[2;5]$, and U_2 would be 2-transitive. Hence, since at least one transposition belongs to U_2, we would have $U_2 = S_8$.

This means that U_2 admits two orbits of lengths 3 and 5, and we may assume that

$$U_2 = \mathrm{Sym}\{1,2,3\} \times \mathrm{Sym}\{4,5,6,7,8\}.$$

Then U_1 contains a 6-cycle and is 3-transitive. But it is well known that a k-transitive group of degree n, with $k > n/3$ contains A_n (see [6, p. 154]). Then $U_1 \geqslant A_8$ and, since U_1 contains also odd permutations, we arrive at $U_1 = S_8$, a final contradiction.

3 The general case

The main idea in excluding the groups S_n for large n will be to show that if U_1, U_2 define a covering of S_n, then one of these subgroups is necessarily primitive and contains a cycle of relatively small prime length. We can then appeal to (2.3). The arithmetic source for such a cycle is the following result that is a slight generalization of Bertrand's postulate:

Lemma 3.1. *For every integer $n \geqslant 8$, there exists a prime p such that $n/2 < p \leqslant n-3$. If $n \geqslant 9$ and $n \notin \{10, 14\}$, then we can choose p such that $n/2 < p \leqslant n-4$.*

Proof. Let $\pi(x)$ denote the number of primes $\leqslant x$. If $x \geqslant 4000$, then [4] implies that

$$\pi(2x) - \pi(x) > \frac{\log 2}{\log 30} \cdot \frac{x}{\log 2x} > 10.$$

Hence the result is clearly true for $n \geqslant 8000$. A direct check of the remaining cases proves the statement.

The previous result will be used in the following context:

Lemma 3.2. *Let U be a transitive subgroup of S_n containing a cycle of prime length p such that $n/2 < p \leqslant n-3$. Then $U \geqslant A_n$.*

Proof. Let Δ be a non-trivial block of imprimitivity. By the transitivity of U, the cardinality $|\Delta|$ is a proper divisor of n. Hence $|\Delta| \leqslant n/2 < p$. However in this case the cycle of length p cannot act faithfully, a contradiction. Thus the action of G is primitive, and (2.3) yields that $U \geqslant A_n$.

Lemma 3.3. *Assume that the symmetric group S_n is covered by the conjugates of its proper subgroups U_1 and U_2. If $n \geqslant 8$, then neither of these subgroups is the alternating group A_n.*

Proof. By way of contradiction, assume that $U_1 = A_n$. Here, (2.1) implies that U_2 contains an odd permutation of every possible type. If n is even, we must have $[n] \in U_2$, so that U_2 is transitive. Let p be a prime such that $n/2 < p \leqslant n-3$. Then $[p;2]$ is an odd permutation type, so that $[p;2] \in U_2$. As $p \neq 2$, this implies that $[p] \in U_2$. By Lemma (3.2), we have that U_2 contains A_n. As U_2 contains odd permutations, we arrive at the contradiction $U_2 = S_n$.

Now let n be odd. Then $[n-1] \in U_2$ and $[n-2;2] \in U_2$. Again, this yields that U_2 is transitive. As in the first case, U_2 contains a cycle of length p, and as above, we arrive at the contradiction $U_2 = S_n$.

The following concludes the proof of the Theorem:

Proposition 3.4. *Let $n \geqslant 9$. Then S_n is not coverable.*

Proof. By (2.1), we may assume that $[n] \in U_1$, so that U_1 is transitive. Let p be a prime such that $n/2 < p \leqslant n-3$. If $[p] \in U_1$, then U_1 contained A_n by (3.2). This, however, contradicts (3.3). Hence we have $[p] \in U_2$. Now consider permutations of type $[p; n-p]$. If U_1 would contain one of these, then taking powers, it would follow that $[p] \in U_1$. But this is a contradiction to (3.2) and (3.3). Hence we must have $[p; n-p] \in U_2$.

If U_2 were transitive, we would have a contradiction by (3.2) and (3.3) again. So U_2 is not transitive. As $[p, n-p] \in U_2$, we obtain that U_2 has precisely two orbits of length p and $n-p$, respectively. In particular, we have $[n-1] \notin U_2$, whence by (2.1), we have $[n-1] \in U_1$. As $[n] \in U_1$, we obtain that U_1 is 2-transitive, and therefore U_1 is primitive.

First, let n be odd. As $[n-2; 2] \notin U_2$, we must have $[n-2; 2] \in U_1$. As $n-2$ is odd, by taking a suitable power, we conclude that $[2] \in U_1$, and (2.3) gives the contradiction $U_1 \geqslant A_n$.

Finally, let n be even. For $n \notin \{10, 14\}$, by (3.1), we can choose the above prime p such that $n/2 < p \leqslant n-4$. Since $[p+2; 2] \notin U_2$, we obtain that $[p+2; 2] \in U_1$. As $p+2$ is odd, by taking a suitable power, we obtain that $[2] \in U_1$. But this is a contradiction as above.

Let $n = 10$. Then $p = 7$ and U_2 cannot contain any permutation of type $[5; 4]$. Thus $[5; 4] \in U_1$, and taking its fourth power yields that $[5] \in U_1$, a contradiction.

If $n = 14$, then $p = 11$. An analogous argument yields $[9; 5] \in U_1$, and $[5] \in U_1$, another contradiction. The proof is complete.

4 Further results

Using similar methods, one can prove an analogous result for the alternating groups. Here, a number of additional subcases have to be considered. For the sake of brevity we omit the proof of the following:

Theorem ([3], [5]). *The alternating group A_n is coverable if and only if $4 \leqslant n \leqslant 8$.*

Using [6, p. 193], it can be seen that the simple groups $\mathrm{PSL}(2, p^f)$ can be covered by the normalizer U_1 of a Sylow p-subgroup and a dihedral group U_2. An inspection of the maximal subgroups of the Mathieu groups shows that M_{11} and M_{12} can indeed be covered. For M_{11}, we can take $U_1 = \mathrm{PSL}(2, 11)$ and $U_2 = M_{10}$, while for M_{12}, the subgroups $U_1 = M_{11}$ and $U_2 = M_{10} : \mathbb{Z}_2$ yield a covering.

Neither the Suzuki groups $\mathrm{Sz}(q)$ nor the sporadic groups M_{22}, M_{23}, M_{24}, Co_1, Co_2, Co_3, J_1, J_2, J_3, Suz, HS, McL, He, HN, O'Nan, Ly and Ru admit a covering. Details may be found in [5].

Added in proof. The first author now has found a classification of groups with a covering by two cyclic subgroups.

References

[1] R. Brandl. A covering property of finite groups. *Bull. Austral. Math. Soc.* **23** (1981), 227–235.

[2] R. Brandl. Integer polynomials that are reducible modulo all primes. *Amer. Math. Monthly* **93**, (1986) 286–288.

[3] D. Bubboloni. Coverings of the symmetric and alternating groups. Preprint. Dipartimento di Matematica "U. Dini", Firenze (1998).

[4] P. Erdös. Beweis eines Satzes von Tschebyschef. *Acta Acad. Sci.* (*Szeged*) **5** (1932), 194–198.
[5] I. Hupp. Polynome, die modulo jeder Primzahl eine Nullstelle besitzen. Diplomarbeit. Universität Würzburg (1991).
[6] B. Huppert. *Endliche Gruppen I* (Springer-Verlag, 1967).
[7] C. E. Praeger. Covering subgroups of groups and Kronecker classes of fields. *J. Algebra* **118** (1988), 455–463.
[8] C. E. Praeger. Kronecker classes of fields and covering subgroups of finite groups. *J. Austral. Math. Soc. Ser. A* **57** (1994), 17–34.
[9] B. L. van der Waerden. Die Seltenheit der Gleichungen mit Affekt. *Math. Ann.* **109** (1934), 13–16.
[10] H. Wielandt. *Finite permutation groups* (Academic Press, 1964).

Received 2 November, 1999; revised 26 May, 2000

R. Brandl, Mathematisches Institut, Am Hubland 12, D-97074 Würzburg, Germany
E-mail: brandl@mathematik.uni-wuerzburg.de

D. Bubboloni, DIMAD, Via C. Lombroso 6/17, I-50134 Firenze, Italy
E-mail: dbubbo@facec.cce.unifi.it

I. Hupp, Mathematisches Institut, Rheinau 1, D-56075 Koblenz, Germany
E-mail: hupp@uni-koblenz.de